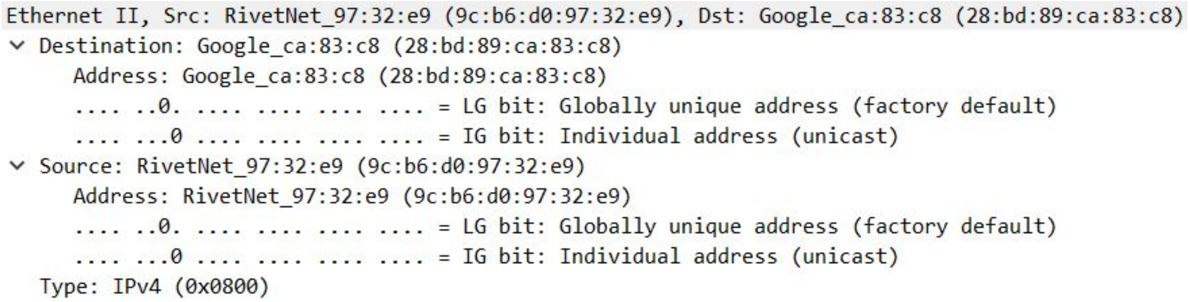
Aleksas Murauskas 260718389
Florence Diep 26072717117
ECSE 416 - Telecommunications Networks
November 9th 2020

Experiment 3 Report - Link Layer

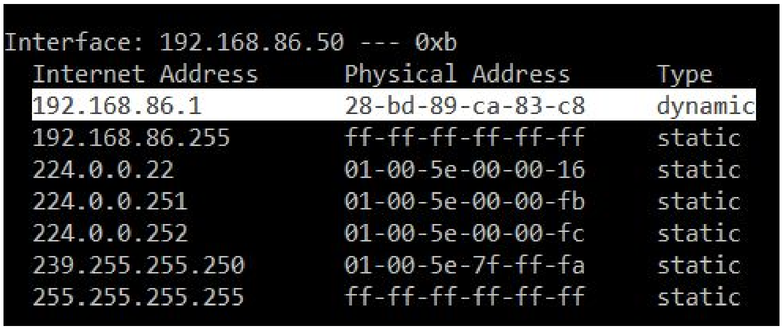
2. Ethernet/Wireless Frames



```
Ethernet II, Src: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9), Dst: Google_ca:83:c8 (28:bd:89:ca:83:c8)
  Destination: Google_ca:83:c8 (28:bd:89:ca:83:c8)
      Address: Google_ca:83:c8 (28:bd:89:ca:83:c8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      Address: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Figure 2.1 - Ethernet II frame of HTTP GET packet

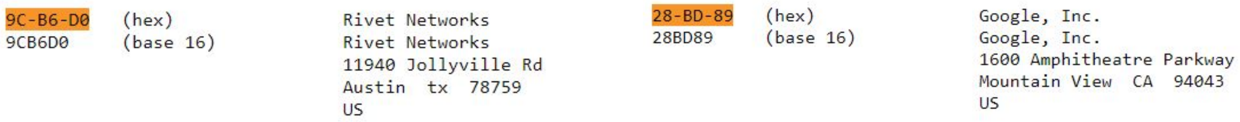
The address of the 48-bit Ethernet address of the laptop being used is 9c:b6:d0:97:32:e9, which can be found in the source portion of the HTTP GET packet as per figure 1 and validated by checking the hardware properties of the WiFi. The 48-bit destination address in the figure is 28:bd:89:ca:83:c8, which is the address of the router and can also be validated by using the ARP command to find its physical address as seen in figure 2. To clarify, the source's IP address is 192.168.86.50.



```
Interface: 192.168.86.50 --- 0xb
  Internet Address      Physical Address      Type
  192.168.86.1          28-bd-89-ca-83-c8     dynamic
  192.168.86.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

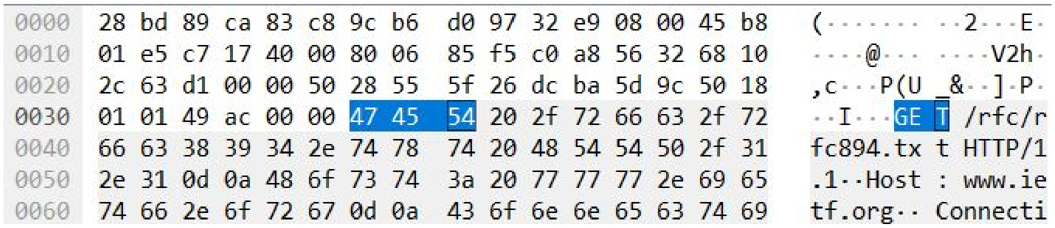
Figure 2.2 - ARP Cache Content for source 192.168.86.50

Figure 3 demonstrates the manufacturers of the Ethernet adapter for both the source and destination. This can be done by searching the first three octets of each MAC address. Additionally, we can see from figure 1 that the hexadecimal value for the two-type TYPE field is 0800, which simply indicates that it is an internet protocol, specifically IPv4. As per figure 2.4, we can see that the ASCII "T" in GET request method appears after 116 bytes in the Ethernet Frame.



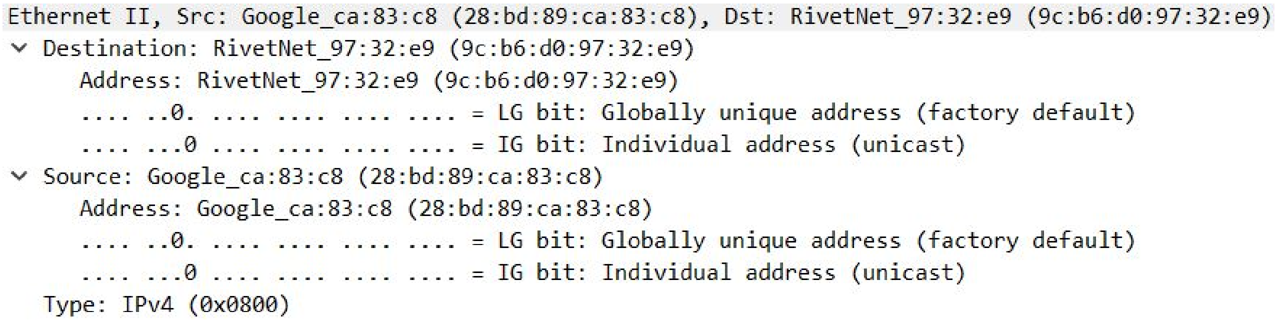
```
9C-B6-D0   (hex)          Rivet Networks               28-BD-89   (hex)          Google, Inc.
9CB6D0     (base 16)      Rivet Networks               28BD89     (base 16)      Google, Inc.
                          11940 Jollyville Rd                                    1600 Amphitheatre Parkway
                          Austin  tx  78759                                      Mountain View  CA  94043
                          US                                                     US
```

Figure 2.3 - Source and Destination Ethernet Adapter Manufacturer



```
0000  28 bd 89 ca 83 c8 9c b6  d0 97 32 e9 08 00 45 b8   (·······  ··2···E·
0010  01 e5 c7 17 40 00 80 06  85 f5 c0 a8 56 32 68 10   ····@···  ····V2h·
0020  2c 63 d1 00 00 50 28 55  5f 26 dc ba 5d 9c 50 18   ,c···P(U _&··]·P·
0030  01 01 49 ac 00 00 47 45  54 20 2f 72 66 63 2f 72   ··I···GE T /rfc/r
0040  66 63 38 39 34 2e 74 78  74 20 48 54 54 50 2f 31   fc894.tx t HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 77 77 77 2e 69 65   .1··Host : www.ie
0060  74 66 2e 6f 72 67 0d 0a  43 6f 6e 6e 65 63 74 69   tf.org·· Connecti
```

Figure 2.4 - ASCII "T" in Request Method GET of Ethernet Frame

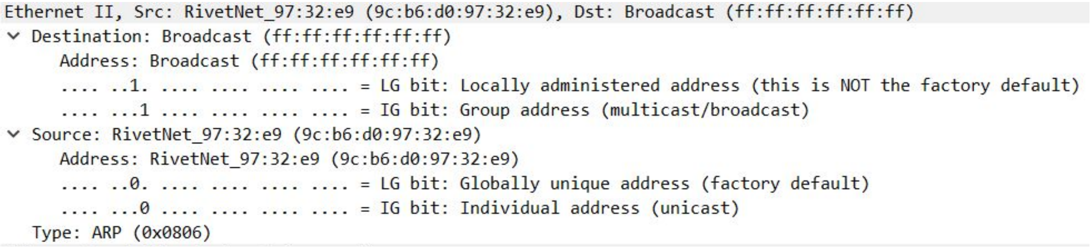


```
Ethernet II, Src: Google_ca:83:c8 (28:bd:89:ca:83:c8), Dst: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
 ⌄ Destination: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      Address: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
 ⌄ Source: Google_ca:83:c8 (28:bd:89:ca:83:c8)
      Address: Google_ca:83:c8 (28:bd:89:ca:83:c8)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: IPv4 (0x0800)
```

Figure 2.5 - Ethernet frame of HTTP Response packet

The value of the Ethernet source address is 28:bd:89:ca:83:c8, which corresponds to the address of the router as seen previously. The destination address in figure 5 is 9c:b6:d0:97:32:e9, which corresponds to the address of the laptop being used.

3. Address Resolution Protocol (ARP)

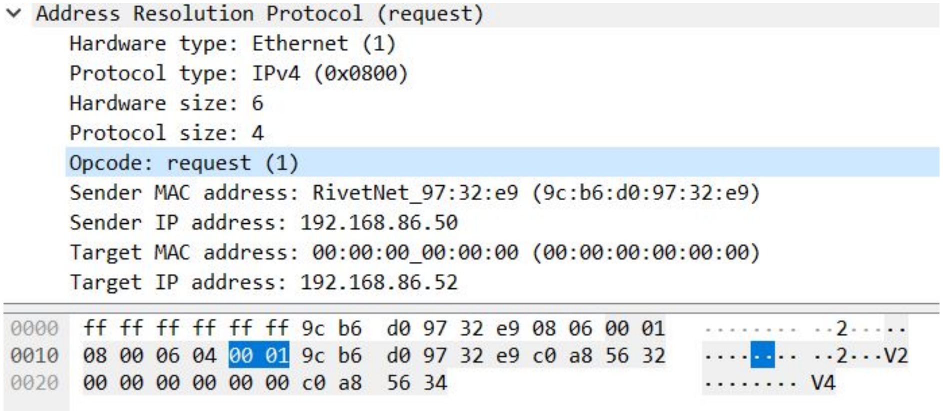


```
Ethernet II, Src: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ⌄ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
 ⌄ Source: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      Address: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: ARP (0x0806)
```

Figure 3.1 - Ethernet II frame of ARP Request Protocol

The hexadecimal values for the source and destination address in the Ethernet frame containing the ARP request message (figure 1) are 9c:b6:d0:07:32:e9 and ff:ff:ff:ff:ff:ff. In this case, the two-byte Ethernet Frame type field is 0806, which indicates an Address Resolution

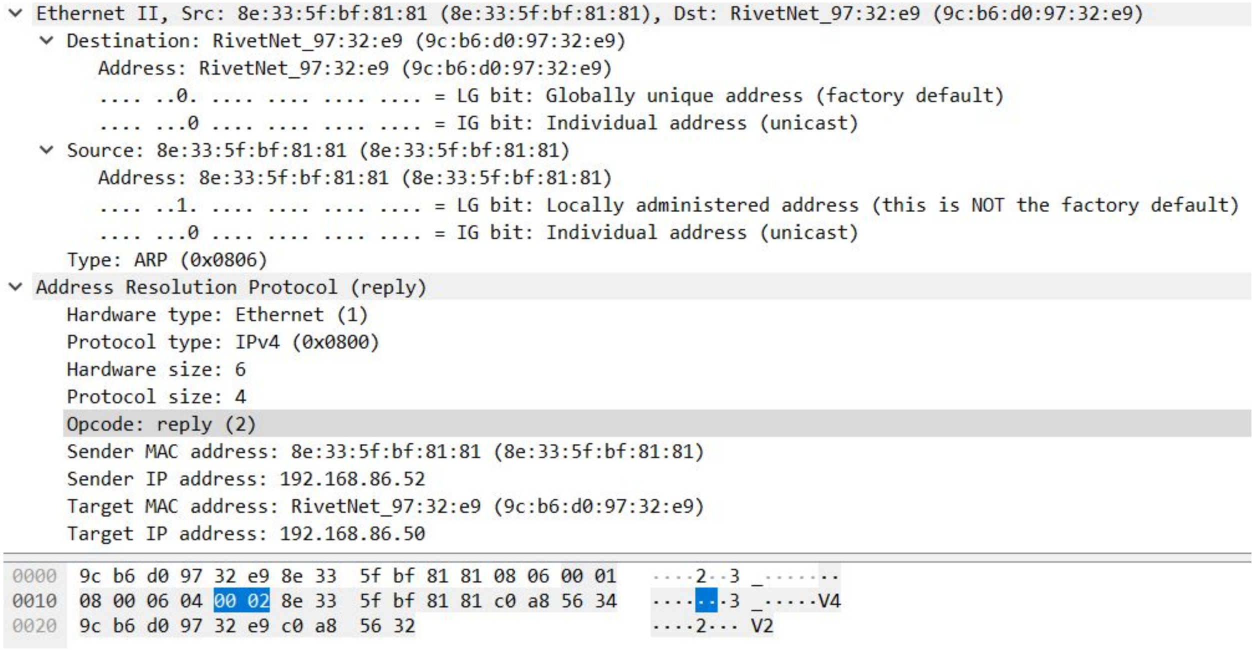
Protocol instead of an Internet Protocol as seen in the previous section, by using the Ethernet broadcast address.



```
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
    Sender IP address: 192.168.86.50
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.86.52

0000  ff ff ff ff ff ff 9c b6  d0 97 32 e9 08 06 00 01   ········ ··2·····
0010  08 00 06 04 00 01 9c b6  d0 97 32 e9 c0 a8 56 32   ········ ··2···V2
0020  00 00 00 00 00 00 c0 a8  56 34                     ········ V4
```

Figure 3.2 - ARP Request Protocol of Ethernet Frame

As seen in figure 3.2, the opcode field begins 20 bytes from the very beginning of the Ethernet frame. The value of the opcode field is 0001 and indicates that the sender is performing a request. We can see that the ARP message contains the IP address of the sender (192.168.86.50). Since it is a broadcast, this request will be sent to all systems contained in the same LAN network. This ensures that when the target system forms an ARP reply, it has a copy of the sender's address and wouldn't require another ARP request. The question appears in the target MAC address in figure 3.2, i.e. 00:00:00_00:00:00.

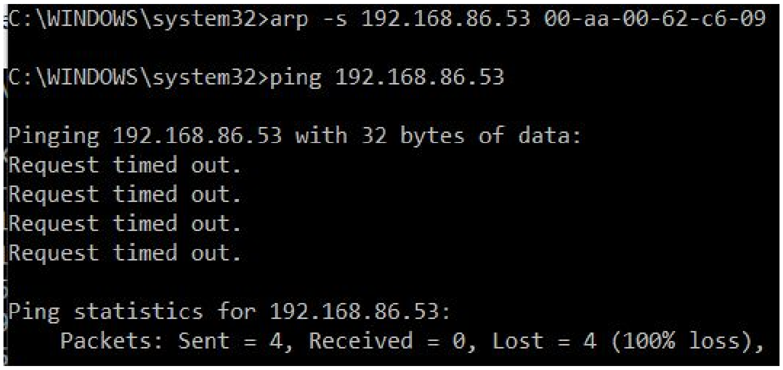


```
v Ethernet II, Src: 8e:33:5f:bf:81:81 (8e:33:5f:bf:81:81), Dst: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
  v Destination: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      Address: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: 8e:33:5f:bf:81:81 (8e:33:5f:bf:81:81)
      Address: 8e:33:5f:bf:81:81 (8e:33:5f:bf:81:81)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 8e:33:5f:bf:81:81 (8e:33:5f:bf:81:81)
    Sender IP address: 192.168.86.52
    Target MAC address: RivetNet_97:32:e9 (9c:b6:d0:97:32:e9)
    Target IP address: 192.168.86.50

0000  9c b6 d0 97 32 e9 8e 33  5f bf 81 81 08 06 00 01   ····2··3 _·······
0010  08 00 06 04 00 02 8e 33  5f bf 81 81 c0 a8 56 34   ·······3 _·····V4
0020  9c b6 d0 97 32 e9 c0 a8  56 32                     ····2··· V2
```

Figure 3.3 - ARP Reply Protocol of Ethernet Frame

Similarly to the ARP request, the opcode of the ARP reply begins 20 bytes from the very beginning of its Ethernet frame and has a value of 0002. This indicates that the ARP is a reply, and we can see its answer to the earlier ARP request in the newly filled target MAC address, i.e. 9c:b6:d0:97:32:e9. The source and destination addresses in the Ethernet frame containing the ARP reply message are 8e:33:5f:bf:81:81 and 9c:b6:d0:97:32:e9 respectively as seen in figure 3.3.

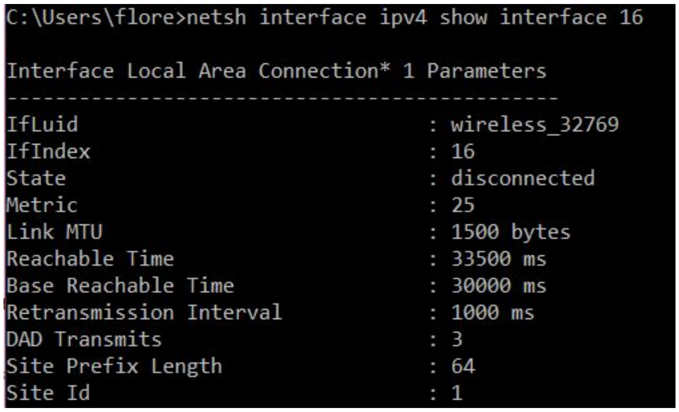
In the event where we manually added an entry to the computer's ARP cache with the correct IP address and incorrect Ethernet address using the arp-s command, the system will fail to reach the given IP address and eventually timeout as seen in the figure below.



```
C:\WINDOWS\system32>arp -s 192.168.86.53 00-aa-00-62-c6-09

C:\WINDOWS\system32>ping 192.168.86.53

Pinging 192.168.86.53 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.86.53:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3.4 - ARP Timeout Example

From the hardware and connection properties, we can determine that the corresponding name to our MAC address is the Local Area Connection 1. In the figure below, we can see that the reachable time is 33.5 seconds, which is our ARP cache timeout. The Windows 10 documentation indicates that the "Reachable Time" value should be between 15 and 45 seconds. A reachable time value outside of that range causes an entry to change to the "stale" state, causing the host to send an ARP request.



```
C:\Users\flore>netsh interface ipv4 show interface 16

Interface Local Area Connection* 1 Parameters
----------------------------------------------
IfLuid                             : wireless_32769
IfIndex                            : 16
State                              : disconnected
Metric                             : 25
Link MTU                           : 1500 bytes
Reachable Time                     : 33500 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 3
Site Prefix Length                 : 64
Site Id                            : 1
```

Figure 3.5 - ARP Refresh Rate

4. Mystery.cap

Within Mystery.cap, all the captured packets are of the protocol Internet Group Management version2 (IGMP). IGMP established multicast group memberships, which are primarily used for one-to-many network applications like streaming,and online gaming. IGMP version 2 has 4 primary message types:

- General membership Query: (0x11) Communicates with all hosts, establishes connection
- Group specific membership query: (0x11 with a specific address) Communicates with the specific group being queried, establishes connection with a specific group
- Membership report:(0x16) Communicates with the specific group being reported. General communication
- Leave Group: (0x17) Communicates with all routers. Shuts down connection.

1. Packet 1: Our first packet is sent to the address 224.0.01 in order to create a multicast group. The type code 0x11 denotes this packet's type as a Membership query. Additionally since the multicast address is 0.0.0.0, there is no specific multicast address, therefore this packet is a general membership query.
2. Packet 2: The Type code is 0x16, therefore this is a membership report query. This means the address specified 239.255.255.250 is added to the multicast group
3. Packet 3: The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.10.10.10 is added to the multicast group
4. Packet 4:The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.3 is added to the multicast group.
5. Packet 5:The Type code is 0x17, therefore this is a Leave group query. The specified address has either timed out or requested to leave the group. In this case the address 225.1.1.3 is removed from the group.
6. Packet 6: The type code 0x11 denotes this packet's type as a Membership query. Additionally since the multicast address is 225.1.1.3, therefore this packet is a specific membership query. The Server is trying to establish a connection with the address that was disconnected in the previous packet.
7. Packet 7: The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.4 is added to the multicast group.
8. Packet 8: The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.4 wants to remain in the group.
9. Packet 9: The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.4 wants to remain in the group.

10. Packet 10: The Type code is 0x17, therefore this is a Leave group query. The specified address has either timed out or requested to leave the group. In this case the address 225.1.1.4 is removed from the group.
11. Packet 11:The type code 0x11 denotes this packet's type as a Membership query. Additionally since the multicast address is 225.1.1.4, therefore this packet is a specific membership query. The Server is trying to establish a connection with the address that was disconnected in the previous packet.
12. Packet 12:The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.5 is added to the multicast group.
13. Packet 13: The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.5 wants to remain in the group.
14. Packet 14:The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.5 wants to remain in the group.
15. Packet 15: The type code 0x11 denotes this packet's type as a Membership query. Additionally since the multicast address is 0.0.0.0, there is no specific multicast address, therefore this packet is a general membership query.
16. Packet 16:The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.5 is added to the multicast group.
17. Packet 17: The Type code is 0x16, therefore this is a membership report query. This means the address specified 239.255.255.250 is added to the multicast group
18. Packet 18: The Type code is 0x16, therefore this is a membership report query. This means the address specified 225.1.1.5 is added to the multicast group